Allens

In alliance with Linklaters

Connected Infrastructure

Unlocking smarter, more liveable cities

To meet the demands being placed on our cities and maintain the liveability, amenity and level of services we have grown to expect, Australia needs to:

1. optimise existing infrastructure assets in the short-to-medium-term; and
2. enable next generation technology in the medium-to-long-term.

Connected infrastructure – using sensors, intelligent systems and other technology to allow for real-time feedback for both governments and citizens – will be central to unlocking a sustainable future.

Opportunities to invest in connected infrastructure and leverage the data generated are significant, but come with risk.

KEY TAKEAWAYS

Governments and organisations can take advantage of the opportunities of connected infrastructure and alleviate the risks by:

1. **SPOTTING DATA COMMERCIALISATION OPPORTUNITIES AND KEEPING ABREAST OF RELEVANT DATA LAWS** – negotiating appropriate rights to access and commercialise data collected through connected infrastructure projects, while keeping an eye on shifting privacy, surveillance and data-sharing laws.

2. **TAKING ADVANTAGE OF 'CORE-PLUS' INVESTMENT OPPORTUNITIES** – identifying the value of 'core-plus' investments and 'future-proofing' these investments by building flexibility into contracts to account for technology evolution.

3. **ENSURING THE SECURITY OF CONNECTED INFRASTRUCTURE** – implementing robust security measures to protect against potential security vulnerabilities and enable prompt detection, investigation and remediation of potential infrastructure attacks.

4. **PREPARING FOR 5G** – considering opportunities for involvement in the rollout and commercialisation of the 5G network and ensuring connected infrastructure projects currently being designed and built can capitalise on 5G when it arrives.

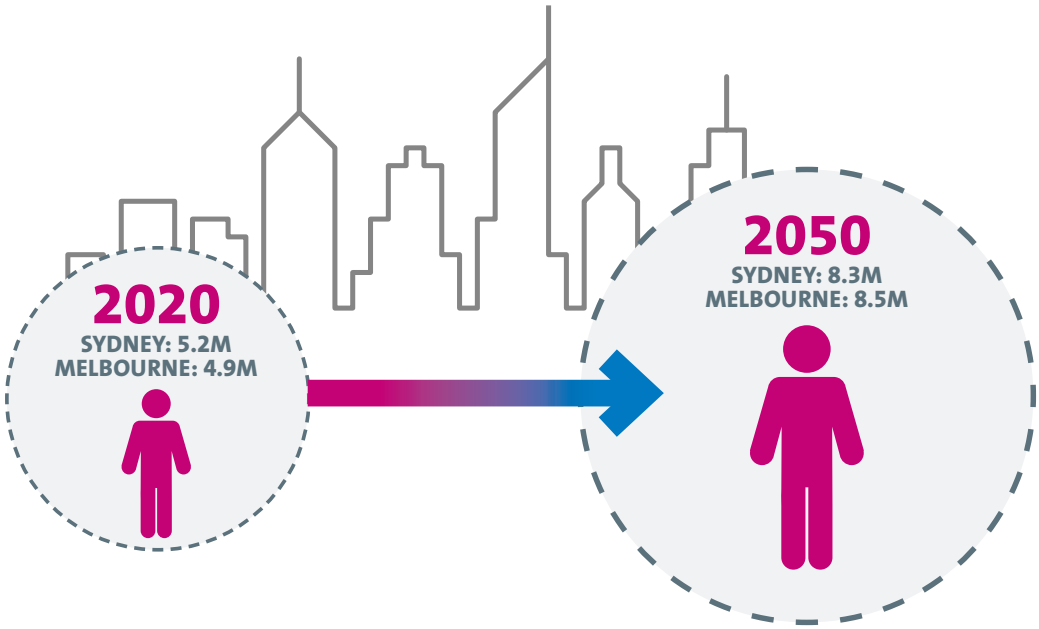
WHO NEEDS TO KNOW ABOUT THIS?

- Infrastructure developers;
- organisations looking to invest in or finance infrastructure projects; and
- government agencies looking to procure the delivery of infrastructure projects.

WE NEED TO FIND WAYS OF OPTIMISING EXISTING INFRASTRUCTURE ASSETS AND LEAD A STEP CHANGE TO UNLOCK NEXT GENERATION TECHNOLOGY.

Rapid urbanisation and population growth have placed our cities under significant strain. Sydney and Melbourne are already under considerable pressure, and – even under a 'medium-growth model' – both cities are expected to reach the size of New York City by 2050.[1] It is estimated that the share of the world's population living in urban areas will rise from 54% in 2019[2] to 68% by 2050.[3]

Both Sydney and Melbourne are expected to reach the size of New York City by 2050



Using 'internet of things' (***IoT***) technology, such as sensors and smart metering, can generate enormously valuable insights and drive down operational costs for governments and the private sector. For instance, energy suppliers will be able to identify and locate surges, and reduce power during expected down times. Smart roads will communicate with traffic lights and vehicles to optimise traffic. For example, on the M4 motorway in Western Sydney, NSW's first 'smart road', metering and variable signage is already being utilised to manage varying traffic flows.[4] The same will be possible for dams, power plants, electricity stations, telecommunication towers, and public transport. This will allow existing assets to be used more efficiently and cost effectively.

Moreover, many of these technologies are already here. As part of its Smart Cities Plan and in response to the Australian Infrastructure Plan, the Federal Government has pledged initiatives and capital to facilitate the development of smart cities, both metropolitan and regional, across Australia. These smart cities will use real time data and smart technology, allowing governments and Australians to better develop and use infrastructure – eg by working toward '30-minute cities', where citizens can access employment, schools, and critical services within 30 minutes of home.

Those who are across the commercial and regulatory complexities will be best placed to act quickly and harness the opportunities in this space.

HOW GOVERNMENTS AND INDUSTRY CAN CAPITALISE ON THE OPPORTUNITIES CREATED BY CONNECTED INFRASTRUCTURE AND MINIMISE THE RISKS.

1 SPOT DATA COMMERCIALISATION OPPORTUNITIES AND NAVIGATE DATA LAWS

As connected infrastructure becomes more commonplace, it will produce data at an unprecedented rate. These datasets offer huge commercial opportunities and potential revenue streams as the public and private sectors find ways to leverage (and combine) this information to generate new products and services. In Milton Keynes in the UK, the MK Data Hub – a collaborative public / private initiative – is tackling key infrastructure challenges relating to transport, education and water through data collection and sharing from sensors owned by individuals, businesses and government. The Hub has undertaken several initiatives aimed at influencing how much water citizens use, with water availability likely to come under increasing pressure due to climate change and population growth.

To capitalise on the data commercialisation opportunities created by connected infrastructure, governments and the private sector will need to navigate complex privacy and surveillance laws, and ethical questions around how data can – and should – be collected and used.

The recent reactions of Hong Kong demonstrators – cutting down smart lampposts over concerns they could contain facial recognition software[5] – highlight the need to balance technological capabilities with ethical considerations and the central role trust will play.

For example, optical surveillance requires consent under surveillance laws, but also raises a range of ethical questions, complicating a process which is designed to be automated.

In Australia, the current surveillance law framework varies significantly between states and territories, while the use of biometric information is largely regulated by the national *Privacy Act*. This regulatory tapestry can make it difficult for companies to easily roll out IoT infrastructure with monitoring capabilities. Despite the Australian Law Reform Commission's repeated calls for a national scheme to streamline surveillance legislation, we don't see any imminent legislative changes on the horizon.

However, a number of proposed legal changes will potentially support further data commercialisation. These include the introduction of various open data regimes (such as the proposed *Data Sharing and Release Act*) which will pave the way for the private sector to gain increased access to government datasets. Businesses will also need to stay on top of changes to data sharing laws which could implicate their own datasets – ie, there could be situations where private sector information will need to be made available on a deidentified basis, as foreshadowed by the Productivity Commission's Inquiry Report on *Data Availability and Use*.

HOW CAN YOU PREPARE?

To take advantage of data access and commercialisation opportunities in the infrastructure space (and, in turn, protect your own datasets), your organisation will need to:

- explore new ways to utilise existing datasets;
- create data governance frameworks to govern decision making around data use cases in an ethical and compliant manner;
- negotiate appropriate data access and use rights when participating in infrastructure projects;
- navigate the legal landscape governing privacy, surveillance and biometric data to ensure new products and services are rolled out in a legally compliant way; and
- monitor the implementation of data sharing regulations.

2 TAKE ADVANTAGE OF 'CORE-PLUS' INVESTMENT OPPORTUNITIES

The increasing popularity of 'core-plus' asset investments has made it easier than ever to attract financing for connected infrastructure projects.

FOR INSTANCE, the recently listed 360 Capital Digital Infrastructure Fund (ASX: TDI), demonstrates the growing popularity of core-plus investments. The fund targets investments in data centres and fibre connectivity assets, and completed an oversubscribed book build ahead of its IPO, raising $65 million.[6]

As investment opportunities in traditional 'core' assets such as roads and ports have become scarcer, we have seen an increase in institutional investors looking for 'infrastructure-like' opportunities that offer inelastic demand and stable, long-term returns. This has included investments in assets such as data networks, cellular towers, intermodal terminals and logistics centres, land titles registries and smart metering (eg Pacific Equity Partners-backed intelliHub's purchase of Origin's smart metering business for $267 million).[7]

Increasing connectivity offers the potential for existing public infrastructure and municipal services to be digitalised and automated, which will necessitate (and we predict, readily attract) growing investment from the private sector. We also expect to see a rise in governments partnering with the private sector for capital and expertise to uplift and alleviate pressure on existing infrastructure using 'greenfields' technology.

FOR EXAMPLE, Ausgrid recently partnered with battery maker Reposit Power to turn 233 NSW households into 'mini-power plants' – allowing households to lower their energy bills and feed energy into the grid to support periods of peak demand.[8]

HOW CAN YOU PREPARE?

Investors and developers should understand the unique risk profile of these projects, including the potential political, competition and technological risks, eg:

- how do you protect against technology obsolescence over the term of a 30 year investment?
- how do you ensure new data-related products and services will be rolled out in a legally compliant way?

Addressing these issues up front at the point of investment will ensure investors do not pay for revenue streams that cannot ultimately be realised in practice.

3 ENSURE THE SECURITY OF CONNECTED INFRASTRUCTURE

Central to the success and further rollout of connected infrastructure will be the ability to assure governments and the community of the security of the offerings. Not only will this encourage public confidence in projects, but it will also ensure infrastructure providers do not suffer the significant costs of a cybersecurity incident or data breach (eg one data breach involving 1 million compromised records costs as much as US$39.49 million).[9]

Like all digital technologies, connected infrastructure brings with it a wide range of security challenges – especially security vulnerabilities in mobile or cloud interfaces which connect users to infrastructure. These could provide a point of weakness through which hackers may gain access to both the infrastructure and associated data.[10] Similarly, inadequate authentication measures (such as simple passwords or lack of two-factor authentication) in even one device might leave the door open for attacks that can affect the entire network.

These potential security vulnerabilities are particularly concerning given reports of nation-state hackers targeting energy sector assets (including the national grid in the UK and similar incidents in the US, Ukraine and elsewhere).[11] In addition, national security questions have been raised over the use of electronic equipment manufactured overseas for infrastructure assets, as seen in the allegations of Chinese 'spy chips' making their way into server motherboards supplied to US companies such as Apple and Amazon.[12] Given the Australian economy already suffers at least $1 billion in annual costs from the 'ransomware epidemic',[13] it's unsurprising the Australian Government has displayed growing sensitivity around securing public infrastructure.

The *Security of Infrastructure Act* came into force in 2018 with the objective of securing Australia's highest-risk critical infrastructure assets (currently identified as approximately 165 electricity, port, water and gas assets) and their operators against hacking, sabotage and coercion from foreign actors. The key elements of the Act involve:

- maintaining a register of critical infrastructure asset ownership and control; and
- expanding the Department of Home Affairs' information gathering power and ability to issue directions with respect to such assets to mitigate security risks.

Given the potential network and population reach of connected infrastructure projects, we would not be surprised to see the *Security of Infrastructure Act* expanded to cover connected infrastructure assets with the potential to have an equivalent impact on the Australian economy or essential public services. Alongside the *Security of Infrastructure Act*, the Telecommunications Sector Security Reforms were passed in 2017, requiring telcos to act to protect their networks and facilities from unauthorised access and interference. →

HOW CAN YOU PREPARE?

- Government agencies procuring infrastructure with 'smart' capabilities will need to ensure adequate security requirements are built into the request for tender and contractual arrangements (with an ability to uplift these requirements as technology and security threats evolve).
- Organisations should ensure the technological architecture of connected infrastructure projects is secure, and that such projects comply with the rapidly shifting regulatory landscape.
- By prioritising cybersecurity in the infancy of a project, parties can avoid the need to 'retrofit' regulatory compliance and security measures, which can be much more expensive and less effective from a security standpoint.
- Implementing robust security measures will help mitigate the risk of a data breach. In addition, detailed and tested data breach and incident response plans will help mitigate the impact of any cybersecurity incident if it does occur.

← The Foreign Investment Review Board (***FIRB***) has also demonstrated a recent tendency to impose conditions on data access when approving foreign investments in Australian infrastructure (eg by requiring that sensitive data be stored and accessed in Australia, or that cloud service providers be selected from a government pre-approved list). As more connected infrastructure is built, we expect FIRB's scrutiny to increase.

4 PREPARE FOR 5G

As millions of data-intensive IoT devices and utilities enter the market, high-speed networks will be needed to handle the unprecedented volume of machine-to-machine traffic.

The advent of 5G technology in Australia and abroad has the potential to help support the growth of connected infrastructure and smart cities generally by:

- allowing for greater device density (5G can accommodate 1 million connected devices per 38 square miles, compared to just 2000 currently);[14]
- increasing data throughput (ie volume of data transferable from the source to its destination within a given timeframe) by a factor of 10;[15] and
- facilitating lower latency (ie reducing the time it takes to get a response to information sent), enabling the support of mission critical applications such as emergency services.[16]

Not only will the 5G network facilitate the operation of connected infrastructure, but the rollout of the 5G network will also itself require significant additional infrastructure to achieve the same scope of network coverage as 4G.

Approximately 400 times more towers may be needed for 5G which will materially alter our urban landscape. [17]

The reason for this is that small cell sites which use the higher-end frequency of the 5G band can provide increased data throughput, but their signal will not travel as far. A greater volume of these small cells will be needed, as well as additional cells offering a lower end frequency to provide macro signal coverage at lower speeds.

As with any major infrastructure rollout, there will be significant opportunities for infrastructure providers and financiers to participate in the development and construction of the 5G network.

While an Australia-wide 5G network is still some time away, the demand for 5G is already apparent – Australia's first auction of 'space' on the 5G spectrum in late 2018 netted the government approximately $853 million for the 350 spectrum lots sold.

In addition to a national rollout, we may also start to see private 5G networks emerge as different sectors – from mining to healthcare to transportation – seek to take advantage of the benefits of 5G.

HOW CAN YOU PREPARE?

- Network operators may wish to explore network sharing models to offset some of the fixed costs associated with building the network. These arrangements will need to be carefully negotiated to ensure they do not fall foul of potential competition hurdles, and that each party's commercial objectives are satisfied.
- Pending the arrival of 5G, parties utilising connected infrastructure and IoT solutions should build flexibility into their contracts to ensure infrastructure services and utilities improve as the underlying broadband network improves (eg by building a 'continuous improvement' mechanism into service levels and minimum technology requirements). This is particularly important given the typically long-term nature of these contracts.

Endnotes

1 'Population Projections, Australia, 2017 (base) – 2066', Australian Bureau of Statistics (22 November 2018).
2 https://www.statista.com/statistics/270860/urbanization-by-continent/
3 United Nations, '68% of the world population projected to live in urban areas by 2050, says UN', United Nations Department of Economic and Social Affairs (16 May 2018).
4 Helen Masters, 'On the (smart) road: How infrastructure can benefit from IoT', *Computerworld* (17 July 2018).
5 'Smart lamppost toppled to ground by Hong Kong demonstrators over Chinese surveillance fears', *ABC News* (26 August 2019).
6 Yolanda Redrup, 'Factories of the future' tech infrastructure fund poised for IPO', *Australian Financial Review* (28 October 2019).
7 Sarah Thompson and Anthony Macdonald, 'PEP-backed intelliHUB on smart meter march', *Australian Financial Review* (8 November 2018).
8 'Creating a greener future with Virtual Power Plants', Ausgrid (28 March 2019).
9 Larry Ponemon, 'Calculating the Cost of a Data Breach in 2018, the Age of AI and the IoT', Security Intelligence (11 July 2018).
10 Ashwin Pal, 'The Internet of Things – Threats and Countermeasures', CSO, (20 May 2019).
11 Alex Hern, 'State hackers 'probably compromised' energy sector, says leaked GCHQ memo', *The Guardian* (18 July 2017).
12 Jim Finkle, 'US warns businesses of hacking campaign against nuclear, energy firms', Reuters (1 July 2017).
13 David Crowe 'Increasing cyber-crime attacks costing up to $1b a year', *Sydney Morning Herald* (11 April 2018).
14 Andre Smith, 'The IoT Future Demands A Supporting Infrastructure', *Digitalist* (6 April 2018).
15 Ibid pp. 58, 70.
16 Nam Nguyen and Geof Haydon, 'The impact of 5G on network infrastructure', *Infrastructure Magazine* (4 September 2019).
17 Ibid.

CONTACTS

Valeska Bloch
Partner
T +61 2 9230 4030
Valeska.Bloch@allens.com.au

Gavin Smith
Partner, Head of Technology, Media and Telecommunications
T +61 2 9230 4891
Gavin.Smith@allens.com.au

David Donnelly
Partner
T +61 3 9613 8112
David.Donnelly@allens.com.au

Jessica Mottau
Partner
T +61 2 9230 4587
Jessica.Mottau@allens.com.au

Leighton O'Brien
Partner
T +61 2 9230 4205
Leighton.O'Brien@allens.com.au

Nick Ng
Partner
T +61 3 3334 3139
Nicholas.Ng@allens.com.au

Victoria Holthouse
Partner
T +61 2 9230 4303
Victoria.Holthouse@allens.com.au

Michael Morris
Partner
T +61 7 3334 3279
Michael.Morris@allens.com.au

Michael Park
Partner
T +61 3 9613 8331
Michael.Park@allens.com.au

Wendy Rae
Partner
T +61 3 9613 8595
Wendy.Rae@allens.com.au

Jacqui Downes
Partner
T +61 2 9230 4850
Jacqueline.Downes@allens.com.au